Technická norma

Datum 1. října 2021

Ref. Č. MEIA0015

Mondi AG.
Harmonizace standardů Mondi

SPECIFIKACE PRO INFORMAČNÍ A KOMUNIKAČNÍ TECHNOLOGIE (ICT) PRO PROVOZNÍ TECHNOLOGIE (OT)

Obsah

Rozdělovník Mondi, AFRY

Orig.	01.10.2021 / PKa, AFRY	01.10.2021 / EP, AFRY	01.10.2021 / LCa, AFRY	01.10.2021 / LCa, AFRY	Original issue
Rev.	Date/Author	Date/Checked	Date/Approved	Date/Issued	Notes

ZKRATKY

A&E	Alarmy a události
AC	Alarm a podmínky
AC	Střídavý proud
APL	Pokročilá fyzická vrstva
ARP	Protokol ARP
BAS	Systémy automatizace budov
CWS	Norma pro pracovní stanice
DA	Přístup k datům
DC	Stejnosměrný proud
DCS	Distribuovaný řídicí systém
DHCP	Protokol konfigurace dynamického hostitele
DNS	Systém doménových jmen
např.	například
EN	Evropské normy
EU	Evropská unie
FE	Funkční / Telekom. uzemnění
GDS	Globální rozřazovací server
HA	Přístup k historii
HART	Dálniční adresovatelný dálkový převodník
HAD	Přístup k historickým datům
HMI	Rozhraní člověk-stroj
I/O	Vstup/výstup
ICMP	Protokol Zpráv řízení sítě Internet
ICT	Informační a komunikační technologie
ID	Systém detekce narušení
IEC	Mezinárodní elektrotechnická komise
IEEE	Ústav elektrotechnických a elektronických inženýrů
IGMP	Internet Group Management Protocol
IoT	Internet věcí
IP	Internetový protokol
IPS	Systém prevence narušení
ISA	Mezinárodní společnost pro automatizaci
ISO	Mezinárodní organizace pro normalizaci

KMS	Služba správy klíčů
KVM	(polní připojení k těmto systémům musí být IP KVM)
LAN	Místní síť
LEED	Vedoucí postavení v oblasti návrhů pro energetiku a životní prostředí
LTE	Dlouhodobý vývoj
NFC	Komunikace v blízkém poli
NIC	Řadič síťového rozhraní
NTP	Protokol síťového času
NTS	Síťový časový server
ONVIF	Open Network Video Interface Forum
OPC UA	Unifikovaná architektura Open Platform Communications
OSDP	Otevřete protokol zařízení pod dohledem
OT	Provozní technologie
PE	Ochranné uzemnění
PN/PN	Profinet/Profinet
PoE	Napájení přes Ethernet
PTP	Přesný časový protokol
RMON	Vzdálené monitorování
SAT	Přejímací zkouška místa
Scada	Dohledová kontrola a sběr dat
SIA	Asociace bezpečnostního průmyslu
SIS	Bezpečnostní přístrojový systém
SNMP	Jednoduchá správa sítě
SPE	Ethernet s jedním párem
TCP	Protokol řízení přenosu
TN-S	Terra Neutral Separate
TSN	Časově citlivé sítě
UDP	Protokol datagramu uživatele
UPS	Nepřerušitelný zdroj energie
VDC	Voltů stejnosměrného proudu
VLAN	Virtuální místní síť
WiFi	Bezdrátová věrnost
XML	Rozšiřitelný značkovací jazyk

1 OBECNÉ

1.1 Účel

Tento dokument definuje obecné principy pro informační technologie použité v systémech provozní technologie. Tento dokument popisuje aplikaci standardních technologií a postupů a konkrétní pokyny a popisy jsou uvedeny v samostatných specifikacích pro každý systém. Mezi takové systémy patří například:

- Scada,
- DCS
- SIS
- Ovladače strojních zařízení nebo aktuátorů (cyber fyzický systém)
- zabudované ICT
- řízení výroby
- systémy sledování provozu
- systémy pro správu budov
- správa údržby
- datová síť

Všechny výše uvedené systémy (a další podobné systémy) budou v tomto dokumentu nazývány systémy.

Tento dokument je určen pro všechny Dodavatele, kteří dodávají systémy, ve kterých ICT figuruje coby

- vložené řešení,
- aplikace nebo
- služby

samostatně nebo coby součást zařízení, senzorů aktuátorů, zařízení IoT či dalšího balíčku.

Veškeré odchylky od těchto pokynů při návrhu či dodání projektu musí být Dodavatelem ohlášeny a jsou přípustné pouze s písemným schválením Mondi. Výběr použité technologie tam, kde tento předpis dává možnost volby, bude uveden v příslušných dotazech a samostatných projektových pokynech.

1.2 Specifikace systémů

Všechna zařízení musí být v souladu se standardy a pokyny Kupujícího. Veškerá ICT zařízení, software a licence obsažené v systému musí být schváleny Kupujícím. Systémy musí být možno upgradovat a musí mít předvídatelné náklady na životní cyklus.

Továrny jsou v nepřetržitém provozu celý rok. Musí být možné opravit část zařízení, aniž by se přerušily procesy. Zvláštní pozornost je třeba věnovat snadné výměně vadných zařízení a komponent. Tam, kde to je potřeba, se použijí redundantní jednotky, které zajistí odolnost procesu, bezpečnost a hlavně spolehlivost provozu.

1.3 Zákony, předpisy a normy

Návrh a specifikace systémů musí být v souladu s platnými místními zákony a předpisy a vyhláškami a vyjmenovanými zákony a normami.

Dodavatel je povinen se informovat o použitelnosti všech závazných zákonů a předpisů a potvrdit Kupujícímu, že dodaný hardware a software těmto požadavkům odpovídá.

Práce musí být v souladu s normami, doporučeními, ustanoveními a bezpečnostními pokyny, které jsou v současné době platné v místě a normami kupujícího.

V příslušných případech musí být zařízení a instalace v souladu s těmito normami, předpisy a pokyny:

- Doporučení IEEE
- Mezinárodní organizace pro normalizaci (ISO)
- Mezinárodní elektrotechnická komise (IEC)
- Evropské normy (EN)
- Mezinárodní společnost automatizace (ISA)
- Vedoucí postavení v energetickém a environmentálním designu (LEED)
- Zákony a předpisy, které jsou v současné době platné v umístění lokality
- Předpisy a doporučení místních úřadů
- Projektové pokyny (budou částečně dodány v průběhu projektů)
- RoHS 3 (EU 2015/863)
- Místní zákon o zdravotním postižení / přístupnosti

1.4 Reference

EN 50173	Informační technologie, Obecné kabelové systémy
EN 50174	Informační technologie. Instalace kabelového systému
EN 50346	Informační technologie. Instalace kabeláže. Testování instalované kabeláže
IEC 60269	Nízkonapěťové pojistky
IEC 60364-5-54	Nízkonapěťové elektroinstalace - Část 5-54: Výběr a montáž elektrických zařízení - Uzemňovací zařízení a ochranné vodiče
IEC 61131-3	Programovatelné regulátory - Část 3: Programovací jazyky
IEC 61499	Funkční bloky
IEC 61850	Komunikační sítě a systémy pro automatizaci energetických společností
IEEE 1588	Standard pro protokol Přesné synchronizace hodin pro síťové měřicí a řídicí systémy
IEEE 802.1p	Přísná priorita
IEEE 802.1Q	Standard pro místní a metropolitní sítě - mosty a přemostěné sítě

MEIA0002	Doporučení výrobci elektrických a přístrojových zařízení
OT-SP_v1.1a	Politika bezpečnosti OT kategorie "A", Mondi Group IM
OT-TS_PROFINET_v1	Technická norma PROFINET, Mondi Group IM

2 ROZSAH SYSTÉMŮ

Rozsah systémů je upřesněn v technických a obchodních specifikacích smlouvy nebo objednávky. Technické specifikace zahrnují seznamy zařízení, software a licencí systémů s hranicemi dodávky a diagramy hranic dodávky.

3 DOPORUČENÍ VÝROBCI

Dodaná zařízení budou v souladu se samostatným standardem Doporučení výrobci elektrického a instrumentačního vybavení (MEIA0002).

4 ROZVOD NAPÁJENÍ A UZEMNĚNÍ

4.1 Rozvod napájení

Přívod proudu bude 400/230 V 50 Hz, systém TN-S.

Nepřerušované napětí bude distribuováno z centralizovaných, redundantních jednotek UPS přes speciální napájecí síť pro UPS. Jednotky UPS budou připojeny k datové síti (IP) a budou sledovány.

4.1.1 Vnitřní rozvod proudu v systémech

Vnitřní rozvod proudu v systémech bude koordinován s návrhářem elektrických systémů Kupujícího, aby se zachovala selektivita síťové ochrany. Obecně bude křivka vypínacího proudu miniaturních jističů v systému Typu B. Případně interní pojistky budou v souladu s IEC 60269 (pojistky nízkého napětí) gG a vypnutí za méně než 0,2 s při přívodu proudu z UPS a méně než 0,4 s v případech bez UPS.

Servisní napájecí kabely budou vybaveny proudovými chrániči (typ A, 30 mA).

4.1.2 Rozvod proudu v systémových místnostech a elektrických kontejnerech na staveništi

Jako součást rozvodu elektrického proudu bude na každém místě (rozvodna/kontejner, serverovna, místnost se stojany) poskytnut jeden zdroj běžného proudu a jeden redundantní zdroj z tovární jednotky UPS.

Větší systémy s hardwarovými jednotkami budou obsahovat rozvodné skříně napájení pro vnitřní rozvod napájení. V elektrických skříních budou integrována nezbytná izolační zařízení a bateriové jednotky, aby se zajistila požadovaná dostupnost a kvalita napájení. Všechny tyto systémy budou obsahovat potřebné spínače, pojistky a/nebo jističe a svorkovnice pro rozvod napájení AC v systému.

Systémy budou obsahovat potřebné spínače, pojistky a/nebo jističe, napájecí jednotky a svorkovnice pro vnitřní rozvod DC napájení systému (pokud nejsou obsaženy v jiných skříních).

4.1.3 Rozvod napájení ve velínech a kancelářích

Ve velínech a kancelářích budou naplánovány a nainstalovány pevné zásuvky pro stolní vybavení (pracovní stanice, telefony, tiskárny atd.) coby součást elektrifikace budovy. Uživatelská zařízení na místě budou připojena ke dvěma zásuvkám samostatně napájeným ze zásuvek rozvodu napájení z jednotek UPS.

4.1.4 Rozvod napájení v polních krytech

Rozvod napájení AC se pro polní kryty naplánuje a nainstaluje zvlášť tak, jak vyžadují sítě, sběrnice, polní zařízení a pomocná zařízení.

4.1.5 Napájení přes Ethernet (PoE)

Pro napájení vybraných zařízení (přístupové body k síti wi-fi, kamery atd.) s datovým spojením přes ethernetový kabel se použije napájení přes Ethernet. Napájení bude probíhat přes aktivní zařízení s aktivovaným napájením přes ethernet. Návrhář datové sítě Kupujícího specifikuje aktivní zařízení, kabelová zapojení a konektory.

4.2 Uzemnění

Obecně vzato se při navrhování uzemnění pro ITC systémy a zařízení musí vzít v potaz pokyny týkající se ekvipotenciálního propojení a uzemnění v budovách se zařízením IT uvedené v IEC 60364-5-54 (Elektrické instalace nízkého napětí – Část 5-54: Výběr a stavba elektrických zařízení – Uzemnění a ochranné vodiče).

4.2.1 Uzemnění v systémových místnostech

Jako součást systému uzemnění a vyrovnávání potenciálu na místě bude poskytnuta jedna PE (ochranné uzemnění) a jedna FE (funkční / telekomunikační uzemnění) přípojnice pro každou systémovou místnost (elektrická rozvodna, serverovna, počítačová místnost,

Elektrická zařízení v systémech ICT budou připojena k místní síti ochranného uzemnění (PE) a funkčního uzemnění (FE). Dodavatel systémů zajistí, aby ochranné uzemnění a uzemnění signálů bylo v jeho zařízeních odděleno.

4.2.2 Uzemnění v krytech v poli

Uzemnění pro kryty v poli se naplánuje a nainstaluje tak, jak vyžadují sítě, sběrnice, polní zařízení a pomocná zařízení. Je nutno řídit se pokyny pro aplikované technologie.

5 SÍŤOVÁ KABELÁŽ A KABELÁŽOVÉ SYSTÉMY

Musí se dodržovat požadavky nařízení a předpisů v normách EN nebo v ekvivalentní standardech týkajících se kabeláže ICT a kabelážních systémů:

- EN 50173, Informační technologie, Univerzální kabelážní systémy
- EN 50174, Informační technologie, Instalace kabelových rozvodů
- EN 50346, Informační technologie, Instalace kabelových rozvodů, Testování kabeláže.

Kabely se vyberou v souladu s normou pro kabeláž MEIA0005.

6 ZÁSADY VYTVÁŘENÍ SÍTÍ

6.1 Připojení k síti pracoviště

Hlavní struktura sítě na staveništi s připojením a podsítěmi je uvedena v samostatném technickém standardu vydaném objednatelem pro strukturu, podsítě a adresování OT ICT.

6.2 Zařízení připojená k síti

Nastavení sítě všech systémů a zařízení připojených k síti musí být dohodnuto s kupujícím a schváleno kupujícím.

Všechny systémy, pracovní stanice a servery musí být synchronizovány s časovým serverem kupujícího pomocí protokolu NTP (Network Time Protocol). Požadovaní klienti NTP musí být zahrnuti do systémů. Síťový časový server (NTS) bude součástí systémů kupujícího.

Pro časově kritické systémy vyžadující zpoždění pod mikrosekundu v geograficky distribuovaných systémech se použije protokol přesného času (PTP) IEEE 1588 (Standard for Precision Clock Synchronization Protocol for Networked Measurement and Control Systems).

Běžné karty adaptéru Ethernet musí mít rychlost 10/100/1000 Mb/s (automatické snímání s možností uzamčení volby) a musí být vybaveny konektory RJ45 pro kroucenou dvojlinku. Musí existovat možnost používat síťové karty s kapacitou 10 GB.

Servery musí být vybaveny kartami Ethernet se dvěma porty pro redundantní připojení k síti (teaming).

6.3 Bezdrátové připojení

Všechny bezdrátové síťové systémy (Wifi) musí používat bezdrátové sítě implementované kupujícím.

Zvláštní bezdrátová řešení související s bezpečností a ochranou musí být zajištěna a realizována podle směrnic pro použité řešení. Viz také Politika OT-bezpečnosti kupujícího pro lokality kategorie "A" (OT-SP_v1.1a).

Komunikace využívající rádiové frekvence musí být realizována tak, jak je popsáno v samostatné technické specifikaci vydané zadavatelem pro bezdrátovou místní komunikaci.

6.4 Protokoly a komunikace

Na síťové vrstvě se používá protokol IP (a ARP), který poskytuje mechanismus pro adresování a správu datových paketů odesílaných do uzlů v síti.

Na transportní vrstvě se pro řízení služeb na aplikační úrovni mezi uzly sítě používá protokol TCP (a podle potřeby UDP, ICMP a IGMP).

Ve všech systémech se používá protokol IPv4, služby IPv6 jsou ve všech síťových zařízeních a uzlech zakázány.

Použití jiných protokolů se dohodne zvlášť (zejména u vestavěných zařízení a strojních zařízení).

6.5 Dílčí sítě

6.5.1 Virtuální sítě LAN

Virtuální sítě LAN musí být realizovány tak, jak je popsáno v samostatné technické specifikaci vydané zadavatelem pro strukturu, podsíťování a adresování OT ICT.

6.5.2 IP adresy

IP adresace musí být realizována tak, jak je popsáno v samostatném technickém pokynu vydaném Objednatelem pro technický standard pro strukturu, podsíťování a adresování OT ICT pro provozní technologie ICT.

6.6 Správa sítě

Síťové komponenty musí mít vestavěné agenty RMON (Remote Monitoring) umožňující centralizovanou správu a diagnostiku sítě pomocí protokolu SNMP (Simple Network Management).

Pro každý přepínač bude kupujícím zřízena samostatná VLAN pro správu sítě, aby byl provoz správy izolován, zabezpečen a upřednostněn. Pokud řešení zahrnuje aktivní zařízení, dodavatel je nakonfiguruje tak, aby podporovalo centralizovanou správu sítě podle pokynů kupujícího. Nesmí se používat nespravovaná síťová aktivní zařízení.

Používá se pouze software a nástroje pro správu sítě dodané kupujícím.

7 VYTVÁŘENÍ SÍTÍ

Datové sítě jsou rozděleny systémem firewall na samostatné části. Pro každé zařízení připojené k síti, které komunikuje v jiném segmentu sítě, je třeba podporovat používání firewallů nebo podobných postupů.

7.1 Správní sítě

Administrativní část sítí se skládá z funkcí potřebných pro standardní kancelářské činnosti, jako jsou telefonní a multimediální služby a připojení k osobním bezdrátovým terminálům.

Mobilní komunikační zařízení musí vždy komunikovat prostřednictvím přístupových bodů ve správních sítích.

7.2 Bezpečnostní sítě

Část bezpečnostních sítí se skládá z funkcí potřebných pro bezpečnostní a dohledové činnosti, kde jsou propojeny bezpečnostní monitorovací a kontrolní systémy, jako je kamerový systém na místě, kontrola přístupu a systémy detekce narušení.

Síť související s bezpečností pracoviště musí být založena na Ethernetu a musí používat spravovatelné "komerční hotové" zařízení a software pro Ethernet. Síťový systém musí zahrnovat ustanovení pro použití redundance, jaká se používá ve standardních ethernetových aplikacích.

Mezi přepínači systémové sítě, řídicími jednotkami, kamerami, operátorskými stanicemi, propojovacími zařízeními a dalšími jednotkami systému musí existovat redundance na fyzické vrstvě. K přepnutí na redundantní trasu musí dojít automaticky, pokud je v používaném kanálu zjištěna porucha komunikace. U všech zařízení musí být k dispozici diagnostika, která indikuje stav sítě, včetně stavu redundantních cest.

Síťová aktivní zařízení musí podporovat kvalitu služby podle IEEE 802.1Q (Standard pro místní a metropolitní sítě - mosty a přemostěné sítě) a prioritizaci podle IEEE 802.1p (Strict Priority) s 8 úrovněmi priority.

Více informací o správě sítě z bezpečnostního hlediska naleznete na samostatných stránkách OT-Security Policy Category "A" (OT-SP_v1.1a).

7.2.1 Video systémy

Video zařízení, software a funkce musí splňovat nejnovější specifikace profilu ONVIF, aby byla zajištěna kompatibilita.

7.2.2 Fyzická kontrola přístupu a uzamykací systémy

Komunikace s prostředím dveří (řídicími jednotkami) musí probíhat pomocí sítě IP. Komunikace s dveřním příslušenstvím (čtečkami atd.) z řídicí jednotky musí probíhat pomocí nejnovější verze protokolu OSDP (Open Supervised Device Protocol) společnosti SIA.

Mobilní přístupové a zamykací pověření musí být pomocí NFC nebo Bluetooth k zámkům nebo čtečkám kontroly přístupu.

7.3 Kritické sítě související s výrobou

Kritické sítě jsou součástí sítí, které zahrnují funkce potřebné pro provozní technologie výroby.

Síť související s komunálními službami musí být založena na Ethernetu a musí používat spravovatelné "komerční hotové" zařízení a software pro Ethernet. Síťový systém musí zahrnovat ustanovení pro použití redundance, jaká se používá ve standardních ethernetových aplikacích.

Mezi přepínači systémové sítě, řídicími jednotkami, operátorskými stanicemi, propojovacími zařízeními a dalšími jednotkami systému musí existovat redundance na fyzické vrstvě. K přepnutí na redundantní trasu musí dojít automaticky, pokud je v používaném kanálu zjištěna porucha komunikace. U všech zařízení musí být k dispozici diagnostika, která indikuje stav sítě, včetně stavu redundantních cest.

Síťová aktivní zařízení musí podporovat kvalitu služby podle IEEE 802.1Q (Standard pro místní a metropolitní sítě - mosty a přemostěné sítě) a prioritizaci podle IEEE 802.1p (Strict Priority) s 8 úrovněmi priority.

Komunikace mezi různými stroji a ostatními řídicími systémy se provádí pomocí datových sítí, Ethernetu s příslušnými protokoly.

Systémová komunikace musí podporovat diagnostiku komunikačních systémů a jejich součástí.

Topologie, kabeláž, materiály a vybavení kritických sítí musí být před realizací schváleny kupujícím.

7.3.1 Řídicí sítě

Řídicí sítě jsou součástí struktury kritických sítí, kde jsou propojeny řídicí systémy procesů a strojů. Je třeba dodržovat technickou normu PROFINET (OT-TS_PROFINET_v1) a samostatné pokyny pro návrh a instalaci řídicích sítí.

7.3.1.1 Řízení procesů

V případě sběrnice I/O nebo síťové funkce zařízení se jako síťový standard upřednostňuje Profinet, EtherNet/IP nebo TSN s OPC UA. Sítě musí být zkonstruovány z ovladatelných aktivních zařízení průmyslové třídy, která jsou schopna odolávat náročným podmínkám prostředí v místě instalace. Aktivní zařízení musí podporovat nezbytné funkce odolnosti sítě. Výběr použité sítě se provede před zahájením návrhu řešení.

Síťová kabeláž a konektory musí být vždy průmyslové kvality a vhodné pro vybrané služby, jak je popsáno v pokynech kupujícího a v platných průmyslových normách.

7.3.1.2 Sítě senzorů a akčních členů

Síť senzorů a akčních členů musí být realizována pomocí použitelné kombinace Profinet, IO-link, APL (Advanced Physical Layer) a SPE (Single Pair Ethernet). Segmenty sítě musí být dimenzovány podle zvláštních pokynů pro projektování, aby byla zajištěna dostatečná rozšiřovací kapacita. Použití sběrnice Profibus na úrovni sítě snímačů a akčních členů musí být zvlášť projednáno a schváleno kupujícím.

Topologie, kabeláž, materiály a vybavení polních sítí na úrovni zařízení musí být před realizací schváleny kupujícím.

7.3.1.3 Konvenční řešení I/O

Přestože se upřednostňuje sériová síťová komunikace, mohou nastat případy, kdy se použijí konvenční I/O systémy. Jednotky I/O musí být samostatně rozdělitelné s

vhodnou ochranou proti vlivům prostředí a musí komunikovat s ostatními systémy prostřednictvím sběrnic Profibus, Profinet, EtherNet/IP nebo TSN s OPC UA.

Standardní signály v zelené oblasti (nové procesní oblasti) jsou:

- Analogové vstupy 4-20 mA, napájení 24 VDC, s HART
- Analogové výstupy 4-20 mA, napájení 24 VDC, s HART
- Diskrétní vstupy a výstupy pro provozní zařízení 24 VDC
- Diskrétní vstupy pro motory 24 VDC (pokud je to možné)
- Diskrétní výstupy pro motory 24 VDC (pokud je to možné)

U projektů typu „brownfield“ se použije stávající komunikační protokol. O tom, jaký komunikační protokol se použije, rozhodne kupující pro každý projekt.

U projektů typu „brownfield“ (stávající technologické oblasti) jsou standardní signály:

- Analogové vstupy/výstupy 4 až 20 mA, napájení 24 VDC, s Hart
  0 až 20 mA DC
  0 až 10 VDC
  0 až 20 VDC

- Diskrétní vstupy/výstupy 24 VDC

Impedance analogových I/O musí být kompatibilní s inteligentními převodníky a polohovadly. Komunikační protokol provozních přístrojů (HART) nesmí narušovat používání měřicího signálu.

Diskrétní vstupy a výstupy musí být galvanicky odděleny a napájeny systémem.

Systém musí monitorovat stav připojení polního zařízení a indikovat poruchy.

7.3.1.4 Řízení strojních zařízení a robotů

Sítě pro balicí stroje a další aplikace typu robotiky a řízení pohybu musí být založeny na řešeních testovaných s vybranými síťovými zařízeními.

7.3.2 Sítě systémů řízení budov

Síťové propojení systémů řízení budov musí být založeno na protokolech pro řízení procesů (jak je uvedeno dříve v tomto dokumentu) nebo na specifických protokolech systémů automatizace budov (BAS) pracujících na síti Ethernet (například Bacnet nebo KNX).

7.3.3 Sítě distribučních systémů elektrické energie

Systémy rozvodu elektrické energie musí být založeny na protokolech definovaných v IEC 61850 (Komunikační sítě a systémy pro automatizaci v energetice), aby se dosáhlo potřebné doby odezvy < 4 ms potřebné pro řízení, synchronizaci, ochranu a měření prvků napájecí sítě, zejména v rozvodně v místě, ale také v jiných částech energetické soustavy.

8 KOMPONENTY PRŮMYSLOVÉ ŘÍDICÍ SÍTĚ

8.1 Síťové přepínače

Aktivní součásti řídicí sítě musí být certifikovány a musí splňovat požadavky vybraných protokolů.

Přepínače musí podporovat automatické vyjednávání (10/100/1000 Mb/s, plný duplex nebo poloduplex).

Spínače musí mít max. 10 µs zpoždění, vyrovnávací paměť min. 12500 bajtů na port.

Typ přepínání určuje hloubku linky. Pokud je požadována hloubka více než 5 řádků, musí být zvolen přepínač s typem přepínání "Cut Through".

Pokud koncové zařízení vyžaduje PoE/PoE+, je třeba podle toho zvolit přepínače.

8.2 Konektory

Konektory RJ45 vhodné pro metodu izolačního posunu (typ Fast connect) se používají v místech s nižšími nároky na prostředí.

Pokud se konektory RJ45 používají pro výrobní účely, musí být vhodné pro průmyslové použití a musí být robustní a v kovovém pouzdře.

Konektory M12 (kódování D) se používají pro síťové kabely vyžadující krytí IP65, tj. pro provozní zařízení ve vlhkém nebo vibrujícím prostředí.

Topologie, kabeláž, materiály a vybavení sběrnic snímačů úrovně zařízení musí být před realizací schváleny kupujícím.

9 KOMUNIKAČNÍ SPOJENÍ

9.1 Obecné

Místo synchronních spojení se v příslušných případech použijí asynchronní typy zpráv.

V případech, kdy je vyžadováno synchronní spojení, musí mít spoje vyrovnávací kapacitu, která pokryje možný výpadek přijímacího konce.

Všechny systémy musí podporovat úplnou transparentnost mezi všemi zdroji informací.

9.2 Komunikace v reálném čase

9.2.1 Komunikace na úrovni sítě 1

Při komunikaci mezi systémy na úrovni řídicích jednotek se používá protokol Profinet over TSN.

V případě, že rozhraní Profinet není k dispozici, použije se například příslušná brána Profinet:

- Modbus-TCP/Profinet

- CAN/Profinet
- Ethernet/IP /Profinet

K oddělení sítí Profinet různých systémů se používají spojky Profinet PN/PN.

9.2.2 Komunikace na úrovni sítě 2 a vyšší

9.2.2.1 OPC UA

Technologie OPC (Open Platform Communications) UA (Unified Architecture) se používá k tomu, aby umožnila aplikacím konzistentní přístup a přenos dat do výrobních systémů a z nich. OPC usnadní integraci systémů ve stávajícím i budoucím heterogenním výpočetním prostředí. Jako upřednostňované řešení se použije nejnovější verze OPC UA (Unified Architecture) s příslušnými informačními modely pro přístup k informacím a průmyslovými standardy. V případech, kdy OPC UA není k dispozici, se použije klasické OPC (DA, HDA, A&E) OPC s bránou OPC UA.

Kompatibilita produktů OPC UA musí být ověřitelná certifikací OPC Foundation.

Podporovány musí být jak serverové, tak klientské aplikace OPC UA. Technická implementace architektury OPC UA musí být před nasazením schválena kupujícím.

Komunikace OPC UA bude zabezpečena pomocí podpory OPC UA Security. Není-li vzájemně dohodnuto jinak, použije se režim zabezpečení Sign and Encrypt. Správa certifikátů instancí aplikací OPC UA vyžaduje podporu serveru OPC UA Global Discovery Server (GDS). Kupující nastaví službu GDS.

Komunikace OPC UA musí používat příslušné standardní profily potřebné pro danou aplikaci, např.:

- Přístup k datům DA
- Přístup k historii HA
- Alarm a podmínky AC

Použití profilů se volí na základě komunikačních potřeb a povahy a dohodnou se na něm komunikující strany.

Datové modely a použití doprovodných specifikací OPC UA (standardní informační modely pro dané odvětví) a specifické informační modely dodavatele schvaluje kupující.

Pro spojení mezi systémy se použije síťové připojení přes firewall kupujícího.

9.2.2.2 Zasílání zpráv

Obecně se pro komunikaci mezi systémy používá komunikace OPC UA s příslušnými datovými modely. V případech, kdy tok informací mezi aplikacemi neprobíhá kontinuálně, ale dávkově, lze použít transakční zprávy.

Řízení front zpráv umožňuje distribuci informací mezi systémy v síti bez ohledu na stupeň jejich propojení. Ke komunikaci stačí pouze přerušované spojení. Pro zajištění komunikace se používají transakční zprávy.

Pro externí zasílání zpráv (mimo síť lokality) se použijí služby připojení kupujícího.

9.2.3 Funkční řízení datového spojení

Opatření týkající se redundance a kontroly stavu spojení se zváží a navrhnou společně s komunikujícími stranami.

Komunikační spojení musí být vybavena hlídači, kteří monitorují stav spojení. Poruchy spojení musí být detekovány a signalizovány alarmem s vysokou prioritou. Součástí je software pro stav a údržbu spojení. Spojení musí být schopno automatického obnovení po obnovení spojení. Při řízení procesů a strojních zařízení musí být k dispozici spolehlivá metoda obnovení bezpečného, kontrolovaného stavu ovládacích prvků.

9.2.4 Odpovědnost za signální rozhraní

Při implementaci systému je dodavatel na své straně odpovědný za realizaci komunikace mezi svým systémem a ostatními systémy. Dodavatel je rovněž povinen bez samostatných pokynů nebo kontroly spolupracovat a spolupracovat s ostatními dodavateli s cílem zajistit plně funkční a funkční rozhraní s vysokou dostupností. V případě provozních závad je dodavatel povinen prokázat bezchybnou funkci svého systému.

Dodavatel odpovídá za testování rozhraní společně s dodavateli komunikujících cizích systémů nejpozději během SAT a před zahájením uvedení do provozu, bez ohledu na dodaný koncový bod (klient nebo server).

10 PROSTŘEDÍ NA MÍSTĚ

Všechny systémy musí být navrženy tak, aby splňovaly požadavky stanovené pro zamýšlené místo instalace. Požadavky na ochranu životního prostředí jsou uvedeny ve specifikacích aplikace, které jsou součástí poptávkové dokumentace každé aplikace. Je třeba se zabývat např. teplotou, vlhkostí, vibracemi, čistotou, prašností a chemickou kontaminací vzduchu.

Kromě toho je třeba pro každou aplikaci zvlášť řešit environmentální otázky související s bezpečností. Takovými otázkami jsou např. hašení požárů a řízení přístupu, které jsou rovněž řešeny v samostatných bezpečnostních politikách.

10.1 Místnosti a prostory

Místnosti a prostory musí být navrženy a vybudovány podle vodítek uvedených v samostatné technické normě vydané zadavatelem pro: skříně, skříňky a místnosti pro provozní technologie ICT.

10.2 Skříně a skříňky

Skříně a skříňky musí být navrženy a vyrobeny v souladu s pokyny uvedenými v samostatné technické normě vydané zadavatelem pro: skříňky, skříňky a místnosti pro provozní technologie ICT.

11 SYSTÉMY

Systémy a zařízení musí být označeny/označeny tak, jak je uvedeno v samostatných technických pokynech vydaných kupujícím.

Systémy a zařízení musí být očíslovány a označeny tak, jak je uvedeno v samostatných technických pokynech vydaných kupujícím.

Pojmenování systému (název hostitele) musí obsahovat předponu specifickou pro danou lokalitu, která odpovídá místu nasazení kupujícího, a musí být v rámci lokality jedinečné. Podrobné pojmenování systému je součástí podrobného technického plánování implementace.

11.1 Pracovní stanice

Výpočetní rozhraní HMI musí být primárně implementováno v prostředí virtualizovaného serveru.

Operátorská rozhraní v řídicích místnostech a mobilní a terénní připojení k těmto systémům musí být IP KVM nebo jednotky tenkého klienta umístěné v uživatelském prostředí, které poskytují pouze požadované funkce.

Pracoviště v řídicích místnostech musí být navržena podle předpokládaného účelu. Na každém pracovišti musí být seskupen určitý počet displejů příslušných velikostí.

Jako uživatelské rozhraní se na staveništi používají standardní komerčně dostupné terénní terminály, mobilní pracovní stanice a podložky nebo ekologicky odolné kiosky.

11.2 Servery a virtuální hostitelé

Výpočetní zdroje se obecně realizují minimálně na dvou samostatných hardwarových platformách (na oddělených místech), které fungují jako horká clusterová jednotka zajišťující odolnost systému v reálném čase.

Servery jsou zpravidla instalovány ve stojanech a skříních v serverovnách. Serverové skříně musí být vybaveny síťovými prostředky umožňujícími centralizovanou správu serverů.

Servery musí být vybaveny minimálně dvěma týmovými síťovými rozhraními, která umožňují komunikaci s uzly systému prostřednictvím dvou samostatných kanálů. Sítě NIC potřebné pro vysokou dostupnost, odolnost proti chybám a zotavení po havárii se specifikují samostatně v závislosti na implementaci.

Servery a virtuální platformy musí podporovat online správu ze strany kupujícího.

O hardwarové konfiguraci serverů se rozhoduje případ od případu podle potřeby a standardů vybavení kupujícího.

11.3 Záloha

Aby bylo možné zvládnout případné hardwarové a softwarové havárie, provádí se zálohování mimo pracoviště. Namísto distribuovaných zálohovacích zařízení se zálohování systémů provádí do datového úložiště připojeného k síti odolné proti

poruchám podle postupů stanovených kupujícím. Musí být k dispozici optimalizace postupů pomocí automatizovaných funkcí, které se starají o včasné zálohování a dostupnost médií s optimálním využitím pracovní síly.

Do postupů automatického zálohování musí být zahrnuty všechny technické typy stanic a serverů, zejména ty s konfigurací systémů a historickými databázemi. Do těchto jednotek musí být možné nahrát záložní prostředky podle norem pro danou lokalitu. Je třeba dodržovat pokyny kupujícího pro ruční obnovu systémů a dat po havárii.

11.4 Tiskárny

Samostatná tisková zařízení a tiskárny (barevný laserový typ) musí být připojeny ke zvláštní samostatné dílčí síti. Tiskárny musí mít prostředky pro obsluhu tiskových front a poskytování standardních tiskových služeb pro všechny systémy připojené k sítím.

Ve vestavěných aplikacích jsou povoleny speciální (termální) tiskárny.

Tiskárny čárových kódů a štítků musí být podle pokynů kupujícího připojeny k segmentu datové sítě v dané oblasti.

Aplikace využívající RFID pro identifikaci musí být podle potřeby definovány v samostatných specifikacích.

12 SOFTWARE

12.1 Obecné

Obecně se dává přednost otevřeným standardům před proprietárními řešeními. Pokud jsou zvolena vlastní řešení, musí to být kupujícímu jasně uvedeno a zdůvodněno.

Veškerý software musí být možné upgradovat na aktualizovanou verzi, zejména v případě nalezených zranitelností nebo jiných chyb softwaru.

Základním jazykem softwaru je angličtina, kterou bude možné rozšířit o další jazykový balíček podle specifikací kupujícího.

Pozornost je třeba věnovat škálovatelnosti, aby systémy byly dostatečně výkonné a zvládaly jak současné požadavky, tak byly snadno přizpůsobitelné budoucím potřebám.

Pokud je software nebo softwarový systém poskytován k instalaci na sdílené klientské nebo serverové počítače, dodavatel jasně uvede požadavky na hardware.

Aplikace, které hojně využívají síťovou komunikaci, musí specifikovat své požadavky na šířku pásma sítě za normálních i rozrušených podmínek.

12.2 Závislosti a licence

Dodavatel musí zdokumentovat veškerý software, který jeho systém vyžaduje a který je dodáván třetími stranami. Musí být poskytnuty kopie licenčních podmínek pro veškerý software třetích stran, který je součástí dodávky dodavatele.

U proprietárního softwaru se přiloží kopie navrhované licenční smlouvy na software.

Licenční politika pro každou aplikaci, zejména s ohledem na konektivitu, musí být jasně a samostatně definována. Generické licence systémového typu nejsou v síťovém prostředí akceptovány. Dodavatel systémů poskytne kupujícímu informace o používaném softwaru s jeho revizemi v exportovatelném formátu (XML nebo obdobném), který bude importován do systému správy majetku kupujícího.

12.3 Operační systémy

Kupující upřednostňuje serverové operační systémy MS Windows Server 2019 (nebo novější). Operační systémy stolních počítačů jsou MS Windows 10 (nebo novější) podle specifikací kupujícího. Licence operačního systému musí být součástí každé pracovní stanice při dodání, pokud není upřednostňováno centrální licencování pomocí KMS-serveru.

Pro řídicí jednotky procesů a strojů, vestavěné řídicí procesory zařízení a další nízko úrovňové systémy jsou akceptovány speciální operační systémy. Dodávky hardwaru, které obsahují vestavěný software, zahrnují právo na bezplatné používání softwaru po celou dobu životnosti hardwaru.

Implementace řízení výroby a dalších činností souvisejících s výrobou musí být založena na standardním produktu MS Windows Server 2019 (nebo novějším). Pro operátorské rozhraní řízení procesů a strojů, programování, správu majetku, diagnostiku a další kancelářské činnosti lze použít také operační systém MS Windows.

Použitelnost služby Windows Active Directory a funkcí musí být samostatně definována ve specifikacích aplikace.

Použití jiných operačních systémů bude projednáno samostatně.

12.4 Standardní software

Kupující používá v kancelářském prostředí standardní balík pracovních stanic CWS (Corporate Workstation Standard), který obsahuje dostupný software a softwarové licence pro různé uživatele. Každá nová pracovní stanice v kancelářském prostředí musí být nainstalována s balíčkem CWS podle pokynů kupujícího.

Všechny systémy a pracovní stanice v rámci služeb souvisejících se staveništěm musí být zabezpečeny tak, jak je uvedeno v technické normě pro kybernetickou bezpečnost vydané objednatelem.

12.4.1 Kancelářské nástroje

Používají se následující standardní formáty kancelářského softwaru:

Zpracování textu	.docx např. MS Word
Tabulkový procesor	.xlsx např. MS Excel
Obchodní grafika	.pptx např. MS PowerPoint
Řízení projektů	.mpp např. MS Project

Přenosný formát dokumentů .pdf např. Adobe Acrobat

Řízení dokumentů podle projektových standardů - bude doporučeno

12.4.2 Systémy CAD

Jako standardní software CAD se používá AutoCAD společnosti Autodesk.

Pro návrh a dokumentaci sítě a softwaru se používá MS Visio s příslušnými aplikacemi.

12.5 Proprietární software

Dodavatelé proprietárních řešení musí specifikovat:

- Historii vývoje produktu
- Aktuální verzi produktu
- Očekávanou životnost a plánované budoucí verze produktu
- Současné úsilí o vývoj produktu
- Podporu produktu
- Politiku dodavatele týkající se aktualizací softwaru a zpětné kompatibility
- Práva kupujícího v případě stažení produktu (např. přístup ke zdrojovému kódu / úschova).

12.5.1 Vlastnictví

Po dokončení implementace systémů budou veškerá práva související s vlastním softwarem převedena na kupujícího.

12.5.2 Preferované technologie implementace

12.5.2.1 Obecné programovací jazyky

- Java,
- C++,
- VB, (C#, VB.Net)

12.5.2.2 Řídicí programovací jazyky,

- IEC 61131-3
- IEC 61499
- Blokové jazyky specifické pro systém

12.5.2.3 Systémy správy databází

- SQL Server
- MS Access (pouze pro jednoho uživatele)

12.5.2.4 Uživatelská rozhraní

- Acrobat Reader
- SAP GUI
- MS Edge

Všude, kde je to možné, by se měla používat tenká webová klientská rozhraní. To má snížit nároky na správu systému.

Obecně platí, že přesnou verzi a revizi (včetně příslušného Service Packu) je třeba konzultovat s kupujícím před implementací v aplikaci.

12.6 Nasazení softwaru

Centralizované nasazení a správa aplikací se upřednostňují tam, kde technologie tenkého webu není schůdným řešením. Dodavatel připraví instalační programy na přenosných discích pro instalaci aplikací klient/server.

13 INFRASTRUKTURA ICT

Obecně platí, že všechny systémy ICT využívají společnou infrastrukturu ICT společnosti Mondi a případně i správu infrastruktury. Patří mezi ně:

- Vzdálený přístup pro podporu/aktualizaci systému
- Segregace sítě a související zabezpečení sítě (firewally, detekce malwaru, IDS, IPS atd.)
- Řízení a monitorování přístupu k síti (kabelové/bezdrátové)
- Prostředí virtuální platformy
- Zálohovací služby
- Ochrana koncových bodů (malware, brána firewall, whitelisting atd.)
- Databáze pro správu konfigurace pro správu majetku
- Inventarizace softwaru a licencí
- Normy pro pojmenování, označování atd...
- Společná spravovaná standardní pracovní stanice
- Společné spravované mobilní zařízení
- Služby správy zranitelností a oprav
- Běžné síťové služby (DHCP, DNS, NTP)
- Správa identit a přístupu (včetně vícefaktorového ověřování)
- Běžné adresářové služby (Active directory)
- Služby ukládání a shromažďování dat ("datová jezera")
- Bezdrátová síť nebo privátní LTE
- Služby bezpečnostního operačního střediska
- Řízení incidentů, požadavků a změn - podpora procesů

Přednostní správu a správu systémových síťových dat, zabezpečení a zdrojů zajišťují weby Windows Active Directory (součást globálních adresářů Objednatele).

Systém webu se podle potřeby aktualizuje o nové systémy a aplikace. Dodavatel připraví svůj systém tak, aby mohl být zařazen do tohoto adresářového systému. Příslušné podrobné definice adresářového systému se zveřejňují a projednávají samostatně.

14 DŮVĚRYHODNOST

Otázky a směrnice týkající se problematiky důvěryhodnosti ICT a systémů jsou uvedeny v politice OT-Security kategorie "A" Sites, Mondi Group IM (OT-SP_v1.1a).

Zvláštní pozornost je třeba věnovat zajištění kybernetické bezpečnosti a dalším otázkám důvěryhodnosti (bezpečnost, soukromí, bezpečnost, spolehlivost a odolnost) systémů a aplikací. Důvěryhodnost je založena na platných postupech hodnocení rizik.

Kupující vydá samostatné pokyny pro realizaci fyzické bezpečnosti pro umístění systémů ICT.

15 POŽADAVKY NA HARDWARE, ŠKÁLOVATELNOST A KOMPATIBILITU

Pozornost je třeba věnovat škálovatelnosti, aby systémy byly dostatečně výkonné a zvládaly jak současné požadavky, tak byly snadno přizpůsobitelné budoucím potřebám. Podrobné požadavky jsou uvedeny v technických specifikacích systémů.

Pokud je software nebo softwarový systém poskytován k instalaci na sdílené klientské nebo serverové počítače, dodavatel jasně uvede požadavky na hardware.

Systémy, které hojně využívají síťovou komunikaci, musí specifikovat své požadavky na šířku pásma sítě za normálních i rozrušených podmínek.

16 POUŽITELNOST, SPRÁVA A PODPORA

Dodavatel popíše administrativní a podpůrné úkoly nutné k zajištění provozu systémů. Dále popíší dovednosti, které jsou pro plnění těchto úkolů vyžadovány od administrativních a podpůrných pracovníků.

16.1 Dostupnost, výkon, monitorování a správa

Dostupnost a údaje o výkonu a ověření každého systému musí být uvedeny v poptávkách po systému a dále ve smlouvách o dodávce. Tyto údaje slouží k ověření výkonnosti a bezchybného fungování systému a/nebo jakékoli jeho části během záruční doby.

Výkonnost aplikace bude monitorována a vykazována pomocí příslušných nástrojů (správa sítě, detekce narušení, monitorování kybernetické bezpečnosti atd.), které poskytne kupující.

Obecně musí všechny uzly systému podporovat protokol SNMP pro správu sítě a monitorování dostupnosti a výkonnosti. Monitorování sítě slouží ke sledování výkonu sítě, odhalování a hlášení problémů a shromažďování informací pro řešení problémů.

Agenti SNMP musí být umístěni v síťových prvcích, aby se hlásili stanicím řízení v síti lokality a odpovídali na jejich požadavky. K ověření dlouhodobé dostupnosti a výkonnosti zařízení a aplikací připojených k síti se používají trvale instalované analyzátory sítě.

Pokud systémy nebo některé jejich části nepodporují vzdálené monitorování SNMP a standardní datové sítě, dohodne dodavatel s kupujícím způsoby vzdáleného monitorování dostupnosti a výkonu.

17 NÁVRH A IMPLEMENTACE SYSTÉMŮ

17.1 Inženýrství

Požadované inženýrské práce v rámci odpovědnosti dodavatele musí být v souladu s dobrými standardy inženýrské praxe.

17.2 Hardwarové inženýrství

Systémová dokumentace musí obsahovat:

- Výkresy a dokumenty pro návrh hardwaru včetně celkových struktur systémů, specifikací a rozvržení hardwaru s identifikací jednotek a označením rezervních míst atd.
- Protokoly a popisy hodnocení rizika důvěryhodnosti a testování zneužití
- Návrh a výkresy rozvodů střídavého a stejnosměrného proudu všech požadovaných zařízení s požadavky na napájení UPS v místě instalace. Před instalací musí být výkresy schváleny kupujícím.
- Návrh a výkresy uzemnění pro každý systém a požadavky na impedanci uzemnění.
- Návrh a výkresy kabeláže mezi různými systémy a rozváděči včetně detailů zakončení kabelů.
- Seznam kabelů a výkresy zakončení pro instalaci.
- Certifikované rozměrové výkresy pro všechny jednotky zařízení, které jsou součástí dodávky.
- Potřebná dokumentace pro instalaci, včetně případných zvláštních požadavků.

Přesný harmonogram dodání dokumentů a časový harmonogram se dohodne zvlášť podle rozsahu projektu a časového harmonogramu.

17.3 Softwarové inženýrství

17.3.1 Obecné

Při dodávkách softwaru a inženýrských činnostech je třeba zohlednit a dodržovat samostatně vydanou politiku OT-Security kategorie "A" Sites, Mondi Group IM (OT-SP_v1.1a).

17.3.2 Specifikace

Všechny softwarové systémy musí být před zahájením implementace plně specifikovány. Použití textových popisů, diagramů, výkresů, prototypů atd. se dohodne případ od případu.

Specifikace musí být ověřena a schválena před zahájením implementace softwaru.

17.3.3 Inženýrství

Před zahájením projektování softwaru musí mít dodavatel schválený plán projektu. To zahrnuje harmonogram projektu, plán kvality, plán obsazení atd.

V plánu kvality dodavatele by mělo být uvedeno, jaké metody hodlá použít k zajištění shody svého softwaru se specifikací.

Dodavatel musí dokončit své vlastní zkoušky před zahájením formálních přejímacích zkoušek (např. tovární přejímací zkouška).

17.3.4 Dokumentace

Vlastní software musí být dodán s dokumentací v příslušných jazycích pro každý z následujících tří účelů:

Uživatelská dokumentace (jazyk webu továrny).

Dokumentace musí umožnit koncovým uživatelům systému jeho používání a efektivní provádění každodenních služeb. Základní uživatelské grafické rozhraní pro monitorování a ovládání musí být v jazyce pracoviště, další systémová hlášení mohou být v angličtině.

Dokumentace pro správu a údržbu (anglicky).

Pokyny se používají pro správce systémů k instalaci systému a jeho údržbě v provozu.

Programová dokumentace (anglicky).

Programy musí být dostatečně zdokumentovány, aby kupujícímu nebo třetím stranám umožnily porozumět programovému kódu a případně jej upravit. To obvykle vyžaduje dokumentaci mimo zdrojový kód a komentáře.